| | | |
|---|---|---|
| LUCAS COUNTY, OHIO<br>BOARD OF COMMISSIONERS | NUMBER: 22b | PAGE 1 |
| TITLE: ELECTRONIC MAIL AND INTERNET USE POLICY | PERSONNEL<br>ADMINISTRATIVE X | RESOLUTION<br>NO: 05-1228 |
| EFFECTIVE<br>DATE: 8/23/05 | TYPE:<br>POLICY X<br>PROCEDURE | SUPERSEDES:<br>POLICY #22a<br>PROCEDURE # |

## I. PURPOSE

This policy is intended to provide guidelines to county employees on the acceptable uses of e-mail, internet, and county network services. The policy further identifies procedures for employees in all county agencies who have elected to use the LCIS managed network to acquire and use e-mail, internet, storage, and other network resources.

## II. DEFINITIONS

A. Department Director: Refers to the head of a department or agency, or the Director's designee.

B. Home Page: The county's information page(s) on the internet/world wide web. The county's home page will contain comprehensive information for the public on county services.

C. Malicious Code: Computer viruses, worms, trojans, malware, malicious mobile code or other programs introduced purposely to disrupt, destroy or damage county information technology.

D. Official Provider: An internet service provider officially selected for use by county departments through a county request for proposal (RFP) or bid process.

E. Authorized User: Employee who has requested and has been authorized internet, e-mail, or county network access from the department director

## III. STANDARDS

A. Official Provider: Official county internet service/e-mail providers will be selected based on standard purchasing policies. A department may use a different service provider if approved by the Data Processing Board based on demonstrated need, but all users must sign an internet request form.

B. Acceptable Use Standards: Acceptable uses for e-mail and the internet will include, but will not be limited to, the following:

B.1 Research/Education: Communication with professional associations, other governmental entities, universities, businesses and/or individuals that facilitate county business, and research and education efforts, as authorized by a department director.

B.2 General Public: Distribution of information to the general public, whereby such information is requested and made available under county guidelines and policies for the release of information and the Freedom of Information Act.

B.3 Incidental Personal Use: Incidental personal use is acceptable if:

- Personal use is limited to personal time during the individual's work day
- Personal use adheres to all other aspects of this policy

C. Prohibited Uses of E-mail and the Internet: Prohibited uses for e-mail and the internet include, but are not limited to, the following:

C.1 Personal Use: Personal use, as stated in B.3, is acceptable when the use complies with the whole of this policy. Personal use does not include solicitation, online gambling, or the distribution of chain letters, jokes, and gossip. Incidental use may include online shopping and other activities related to personal recreation or personal business.

C.1a A use of any other e-mail system other than the county-hosted e-mail system Is prohibited. Use of other e-mail systems may result in the loss of internet access. Exceptions based on business need are to be presented to the Data Processing Board.

C.2 Unauthorized Access: Efforts to gain unlawful or unauthorized access to information, data, computer, and communication resources may result in termination and/or prosecution. Employees are prohibited from using unauthorized passwords, accessing files, retrieving stored communications, disclosing information or e-mail messages unless specifically authorized by the department director.

C.3 Malicious Code: Intentional introduction of, or experimentation with, malicious code such as computer worms or viruses, trojans, or other malware.

C.4 No County Affiliation: Illegal, fraudulent, or malicious activity, political activity, Religious promotion, solicitation, or activity on behalf of organizations or individuals having no affiliation with county business.

C.5 Copyright/Patent Violations: Transmission of materials in violation of applicable copyright laws or patents.

C.6 Work Interference: Sending of messages likely to result in the loss of recipients' work or systems, and other types of use that could cause congestion of the network or otherwise interfere with the work of others.

C.6a The use of streaming video, streaming audio, instant messaging, net meetings, net chat, P2P, or other interactive applications is prohibited. Use of such technology may result in loss of internet access. Exceptions based on business needs are to be presented to the Data Processing Board.

C.6b Downloading software (screen savers, games, utilities, applications, etc.) that is not authorized nor directly related to county business is prohibited. Doing so may result in the loss of internet access. Exceptions based on business needs are to be presented to the Data Processing Board.

C.7 Obscene/Profane: Generating, receiving, viewing, storing, transmitting or other use of data or other matter which is abusive, profane or offensive to a reasonable person. This policy recognizes county law enforcement agencies may have to access such sites as part of their work assignment.

C.8 Harassment: The use of the internet or e-mail to harass employees, vendors, customers, and others is prohibited. This includes any insensitive, derogatory, offensive or insulting messages.

C.9 Aliases: The use of aliases while using the internet is prohibited. Anonymous messages are not to be sent. Also, the impersonation of others, and/or misrepresentation of an employee's job title, job description or position in the county is prohibited.

C.10 Misinformation/Confidential Information: The release of untrue, distorted, or confidential information, as defined by Ohio's Sunshine Laws, regarding county business is prohibited.

D. Costs: The County will fund the official service provider. Departments requesting use of another service provider will be considered based on the following:

D.1 Budgeted: Funding must be available within a department's adopted budget.

D.2 Departmental Regulation: A department director or designated representative will monitor all usage and costs.

D.3 Efficient/Effective Use: Users have selected another online service as the most efficient and cost effective tool in comparison with all other communications tools.

D.4 Additional Costs: No additional internet account costs (e.g. upgrading browsers) may be incurred by a department/user without consent of the department director and/or Data Processing.

E. Legal Issues

E.1 Copyrights: Most of the information available on the internet is copyrighted. It is illegal to reproduce or redistribute copyrighted information regardless of its source. It is the department director's responsibility to ensure that copyrighted information is not misused by employees. Violation of copyright laws endangers the county and legal remedies include large fines.

E.2 Discrimination: Harassing messages derogatory comments, or other forms of discrimination based upon color, sex, religion, creed or disabilities is against the law. It is the department's responsibility to ensure that employees do not engage in discriminatory behavior while accessing the internet. Violation of discrimination laws may result in disciplinary action up to and including dismissal and may include referral of a case to appropriate authorities for civil or criminal prosecution.

E.3 Privacy: Employees do not have a right to privacy while accessing the internet through the use of county property. The county reserves the express right to monitor, in any way, the activities of the employee while accessing the internet.

IV. PROCEDURES

A. Access: A department will register each of its user's names with Data Processing before any outside service is accessed.

B. Usage Request: A user and the user's department director must complete and sign an email/internet services use request before a user name is assigned and access to the internet is allowed on a county-owned account.

C. Remote Access: An employee may access a county account from a remote location other than the site designated for that account (e.g. telecommuting or check e-mail while away from the office on business) with approval of the employee's supervisor and only for county business.

D. Anti-Virus Scans: Files from all outside sources, including the internet, must be scanned by the user or the user's department with anti-virus software before first use. LCIS provides an enterprise-wide anti-virus solution capable of performing the scan. The LCIS Helpdesk at 419-213-4037 can provide guidance on how to accomplish a file scan.

E. Compliance Review: Violations of the internet policy and procedures will be evaluated on a case-by-case basis by the department director. Violations may result in disciplinary action, up to and including dismissal, and may include referral of a case to the appropriate authorities for civil or criminal prosecution.

F. Downloading Files: Downloading files that are directly related to required business need is permitted. The possibility of downloading a file with a computer virus, worm, trojan, or other malware is great, and care must be taken not to contaminate the county's network. All downloaded files should pass an anti-virus scan prior to using the file.

G. Uploading Files: Uploading files that are directly related to a required business need is permitted. The possibility of uploading a file with a computer virus, worm, trojan, or other malware is possible, and care must be taken not to contaminate the receiving party's systems and network. Outbound files should pass an anti-virus scan prior to uploading the file.

H. A user, in forwarding a message which originates from someone else, may not make changes to that message without clearly disclosing the exact nature of the changes and identity of the person who made the changes. If a message has been designated by its originator as confidential or privileged, it may not be forwarded without the written consent of its originator.

I. All internet and e-mail activities occurring on county-provided PC's and network resources are public information unless otherwise exempted by local, state, or federal law.

J. Web Page: To ensure a uniform county web presentation, development of a web or home page for personal or department purposes on the county account must be authorized by the county administrator.

K. Users are responsible for the security of their electronic mail and internet account passwords and any electronic mail or documents that are sent via their account. To protect an account against unauthorized use, take the following precautions:

K.1 Users should log off electronic mail and internet accounts before leaving their computer unattended. If an electronic mail account is left open and someone else uses it, it will appear as if the authorized user sent the message. The authorized user will be held accountable.

K.2 Do not give out your password. You are responsible for messages sent via your account. Correspondingly, do not use or tamper with someone else's account without their knowledge and consent. Unauthorized use of an electronic mail account is in violation of county policy.

K.3 Change your password frequently. Passwords can be stolen, guessed or be inadvertently made available.

K.4 Passwords are to be a minimum of six characters in length and must contain uppercase, lowercase, and one special character.

L. Email Retention: The Lucas County Data Processing Board passed an Email Retention policy on March 3, 2017. As email identifies a format, not content – email as a storage medium is not optimized for long term storage of documents.

L.1 Items contained in email that have identified content that may require a legal retention period must be stored in means outside of email, and for the period identified by Ohio Revised Code (ORC), or by other governing laws or regulations.

L.2 It is expected that every individual agency have an internal policy to address the storage of their critical digital content, email is not a means of storage nor an historical archiving tool.

L.3 The approved email retention period as of January 1, 2018 will be for a period of five (5) years from the creation date (authored or received).

L.4 All email items in excess of five (5) years of age, regardless of content, will be irrecoverably purged from all systems. This includes back-up (tape and other media) and retention systems.

L.5 All requests for email outside of the scope of five (5) years internally or externally, will no longer be able to be satisfied by LCIS. There will be no means, regardless of severity, to satisfy ANY request that falls outside of the scope of five (5) years. This includes but is not limited to; Public Records Requests, Legal Requests, Discovery requests for litigation, Subpoenas, Court Orders, Internal requests, etc.

APPROVED BY: Megan Kilgore DATE: 07/14/2017